Department of Administration's Internet and E-Mail Usage Policy

Introduction

The Internet and e-mail have emerged as valuable and cost-effective tools for DOA employes. However, press reports and court cases from around the country underscore the fact that these technologies can also pose potential problems for both employers and individual employes. DOA's Internet and E-Mail Usage Policy is designed to encourage the appropriate use of the Internet and e-mail, while also minimizing risks.

These guidelines encourage all DOA employes to use common sense when they use the department's Internet or e-mail facilities. While the department has the ability to monitor Internet usage, we do not do so routinely. Our employes are trusted colleagues and are expected to use all business tools appropriately. However, if instances of abuse of Internet access become more prevalent, more active monitoring might be needed. The department will comply with reasonable requests from law enforcement and regulatory agencies for access to logs, diaries, archives and other records regarding any employe's e-mail or Internet activities. All employes using Internet and e-mail resources are also reminded that the department's Internet and e-mail files may be subject to disclosure under the state's public records law.

The department may install filters to block access to inappropriate Internet sites. However, the fact that access to a particular site is not blocked does not necessarily mean that it is an appropriate site.

Guidelines

Employes should contact the Office of Computer Services (OCS) if they have any questions about the following guidelines:

- □ The display of any kind of sexually explicit image or document on any department system, including related "chatroom" conversations, is prohibited and may constitute a violation of our policy on sexual harassment. In addition, such explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.
- □ The display of any kind of offensive image or document on any department system that violates any departmental policies, state laws or federal laws prohibiting discriminatory or harassing activities affecting any protected group is prohibited and may constitute a violation of our policy on harassment or discrimination. In addition, such material may not be archived, stored, distributed, edited or recorded using our network or computing resources.
- ☐ If you find yourself connected unintentionally to a site that contains sexually explicit or other offensive material, you must disconnect from that site immediately.
- □ The department's Internet facilities and other information technology resources may not be used knowingly to violate any applicable laws, statutes or ordinances. Use of any department resources in connection with any illegal activity is grounds for immediate dismissal and it is the policy of this department to cooperate with any legitimate law enforcement investigation of potential criminal activity.

- □ To prevent computer viruses or other potentially harmful computer codes from being transmitted to or through the department's information technology systems, downloading of any software or computer code is prohibited unless explicitly authorized by the manager of the affected system(s). All software downloaded must be registered to and becomes the property of the department.
- Any software or files downloaded via the Internet into the department's network become the property of the department. Any such files or software may be used only in ways that are consistent with their licenses or copyrights. No employe may use the department's Internet or e-mail facilities to knowingly download or distribute pirated software or data. Violations of any software license agreements or information services contracts by the unauthorized duplication of software, files, operating instructions or reference manuals are strictly prohibited.
- □ No employe may use the department's Internet facilities to:
 - Download entertainment software or games, or to play games against opponents over the Internet.
 - Download images, audio files or video files unless there is an explicit business-related use for the material.
 - Upload any software licensed to the department or data owned or licensed by the department without explicit authorization from the manager responsible for the software or data.
 - Deliberately propagate any virus, worm, Trojan horse, trap-door program code or any other code that may interfere with the operation of any information technology system.
 - Knowingly disable or overload any computer system or network, or to circumvent any system intended to protect the privacy, functionality or security of another user.
- □ No employe may use department's Internet or e-mail facilities for personal financial gain or for political activities.
- □ Each employe using the department's Internet and e-mail facilities shall identify himself or herself honestly, accurately and completely (including department affiliation and job classification where requested) when using these resources (for example, when participating in newsgroups or when setting up accounts on outside computer systems).
- Only those employes or officials who are duly authorized to speak to the media, to analysts or in public gatherings on behalf of the department may speak/write in the name of the department to others using Internet or e-mail facilities. Other employes may participate in newsgroups or other electronic forums in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves. Where an individual participant is identified as an employe or agent of this department, the employe must refrain from any unauthorized political advocacy and must refrain from the unauthorized endorsement or appearance of endorsement by the department. Only those managers and department officials who are authorized to speak to the media, to analysts or in public gatherings on behalf of the department may grant such authority to newsgroup participants.

- □ The department retains the copyright to any material created by employes in the course of their official duties, including materials posted to any forum, newsgroup or World Wide Web page by any employe in the course of his or her duties.
- □ Copyrighted materials belonging to entities other than the department may not be transmitted by employes on the department's Internet or e-mail system. All employes obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission, or as a single copy for reference only. Failure to observe copyright or license agreements may result in disciplinary action up to and including termination.
- □ Employes are reminded that newsgroups are public forums where it is inappropriate to reveal confidential information, customer data, and any other material covered by existing department confidentiality policies and procedures. Employes releasing protected information via the Internet or e-mail, whether or not the release is inadvertent, may be subject to disciplinary action under existing data security policies and procedures.
- □ Employes may use the department's Internet and e-mail facilities for non-business research or browsing during their designated lunch time or other breaks, or outside of work hours, provided that it does not interfere with official duties and that all other departmental usage policies are adhered to.
- □ The limited use of information technology resources for personal or charitable purpose during non-work hours is permitted, provided that permission of the employe's supervisor is obtained and that consumable supplies, such as paper goods, are replaced.
- □ The limited use of network messaging services, such as e-mail and the Internet, for the preparation and transmission of personal electronic messages to and from members of the employe's immediate family is permitted, as long as that use does not disrupt official use of the resource.
- □ User IDs and passwords help maintain individual accountability for Internet, intranet and e-mail resource usage. Any employe who obtains a password or ID for an Internet, intranet or e-mail resource must keep that password or ID confidential. The sharing or use of another employe's user IDs or passwords to obtain access to the Internet, intranet or e-mail is prohibited.
- □ The department has installed a variety of firewalls, proxies, Internet address screening programs and other security systems to assure the safety and security of the department's networks. Any employe who attempts to disable, defeat or circumvent any department security facility will be subject to immediate dismissal.
- Computers that use modems to create independent data connections may interfere with our network security mechanisms and can potentially be used by a third party to compromise the department's network security. Any computer used for independent dialup or leased-line connections to any computer or network must be approved by the department and must be isolated from the department's internal networks.

A Few Additional Comments

While these guidelines define how DOA employes can and cannot use the department's Internet and e-mail facilities, they can not cover every conceivable situation. That is why common sense and professional courtesy will still be required. For example, Internet sites can include information or images that are acceptable to some people but not others. The best practice is to err on the side of caution while using these resources. The most publicized examples of inappropriate materials include those with sexually-oriented images, racism and hate speech. These sites may include "jokes" or other offensive messages that are sometimes forwarded via e-mail to coworkers or others. It is obviously unacceptable for such material to be identified as coming from this department.

Material on the Internet does not have to be illegal or patently offensive to be deemed inappropriate for the workplace. Specifically, while limited personal use of Internet and e-mail facilities is allowable, as outlined above, excessive access to non-business related sites (e.g., those that feature sports, stock and other financial data, vacation and travel planning, consumer products, and entertainment) is not allowed.

The guidelines outlined above are intended to cover reasonably foreseeable circumstances, but other uses of Internet or e-mail facilities could violate the Department of Administration's Work Rules, listed in the DOA Employe Handbook. As with any violation of work rules, inappropriate use of Internet or e-mail facilities may be grounds for disciplinary action up to and including discharge.

These work rules prohibit the following:

Work Performance

 Neglecting job duties and responsibilities, loitering or engaging in unauthorized personal business or visiting.

Use of Property

- Abuse or misuse of government or private property, materials or equipment, including motor vehicles.
- Stealing, unauthorized possession or use of government or private property, equipment or materials.
- Unauthorized use of state property or equipment including, but not limited to: vehicles, telephones, telefax machines, copy machines, mail service or computer resources.
- Unauthorized access to the Internet system through state provided gateways in order to conduct private matters.
- Unauthorized installation and/or use of protected software.

Personal Actions and Appearance

- Harassment or discriminatory activities, including creation of a hostile or offensive work environment.
- Immoral conduct or indecency.

In short, while we have set forth explicit guidelines for Internet and e-mail usage, the real issue is finding ways to use all of the department's resources to promote our business goals. That means you should use the Internet and e-mail exclusively for business-related purposes, with the exceptions outlined above. In all circumstances, we insist that you conduct yourself in a businesslike, honest and accountable manner when using these facilities. This includes careful observance of copyright, software licensing and the privacy of others, just as you would in any other business dealings.

NOTE: Certain terms in this policy should be understood expansively to include related concepts. Department includes all of our internal divisions as well as our attached boards, offices and commissions. Internet includes the department's intranet and associated information technology systems. Employe includes any person given access to department Internet, intranet and/or e-mail facilities, including classified and unclassified employes of the state, interns, and limited term employes. This policy also applies to contract staff, although they are not considered employes of the department. Document covers any kind of file that can be read on a computer screen as if it was a printed page, including HTML files read in an Internet browser, any file meant to be accessed by a word processing or desk-top publishing program or its viewer, or the files prepared for the Adobe Acrobat reader and other electronic publishing tools. Graphics includes photographs, pictures, animations, movies, or drawings. Display includes monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions and virtual-reality tools.

All employes granted Internet and/or e-mail access using department facilities will be provided with a written copy of this policy. This policy will also be posted on the intranet so that it is available and conspicuous to employes at all times. In addition, this policy as well as the DOA Employe Handbook will be distributed in the New Employe Orientation seminars conducted by the Bureau of Personnel.

Acknowledgment of Receipt

Department of Administration's Internet and E-Mail Usage Policy

I have a received a written copy of the Department of Administration's Internet and E-Mail Usage Policy. I fully understand the terms of this policy and agree to abide by them. I realize that the department's security software may record for management use the Internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file.

I also indicate my explicit knowledge of the following specific policy items by affixing my initials adjacent to each:

Employe Signature		Date	
Employe Name (Please Print)		Date	
	at any violation of this po may result in criminal p	olicy could lead to dismiss rosecution.	al and that certain
departme the depar material	The display of any kind of sexually explicit image or document on any department system, including related "chatroom" conversations, is a violation of the department's policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.		
stored in	I am aware that the department reserves the right to inspect any and all files stored in public and private areas of our network in order to assure compliance with the policy.		
	re that the department h and record all Internet us	nas software and systems sage	in place that can
	re that the department r communications	outinely monitors usage p	patterns for its
Work Ru Employe policy, th	les, which have been pub Handbook. Although th	E-Mail Usage Policy contablished and distributed to ose Work Rules are re-iteractivities by which an emption of this policy.	employes in the DOA rated within this

Please **SIGN** this acknowledgement and **RETURN** it to the Department's Bureau of Personnel for placement in your personnel file. The Bureau of Personnel is located on the ninth floor of the State of Wisconsin, Administration Building, 101 E. Wilson St., Madison, WI 53702.